AB HANDSHAKE

FRAUD REPORT Q4 2025

ABHANDSHAKE.COM

Q4 2025 FRAUD REPORT BY AB HANDSHAKE

This read pulls together our quarterly findings, explains what each fraud looks like in practice, shares real-world patterns and anecdotes, and closes with practical detection and mitigation advice driven by AB Handshake's AI equipped Fraud Management System.

Telecom fraud never stops, it only changes. Q4 2025 is full of surprising events across our customer base, as we see fraudulent attacks continuing to attempt to break through defenses.

Our Q4 review focuses on the major fraud vectors observed in voice and SMS traffic monitored by AB Handshake Fraud Management System:

THE AB HANDSHAKE SYSTEM – REPORT DATA SOURCE

AB Handshake has created a global system of products and solutions designed to eliminate all forms of voice and SMS fraud.

Altogether, AB Handshake's solutions process over 200 million call attempts daily for more than 160 operators each month.

This report is based on anonymized statistics from AB Handshake's machine learning-powered AI Shield solution, which detects and blocks voice and SMS fraud in real time with an industry-leading accuracy of 99.995 %, < 0.001% false positive rate, and a false discovery rate of < 3%.

This report summarizes all fraud cases detected by AI Shield. All data has been reviewed by the AB Handshake analytical team, visualized and prepared for this report in accordance with data protection policy.

THE REPORT INCLUDES INFORMATION ON A SELECTION OF THE FOLLOWING FRAUD TYPES:

IRSF

International Revenue Share Fraud (IRSF). A type of voice fraud that involves the artificial inflation of a revenue share number that the fraudster will gain profit from. Different fraud methods are used to commit IRSF, and can include PBX Hacking, Wangiri, Wangiri 2.0, P2S fraud, etc.

PBX HACKING

A voice fraud method where fraudsters gain unauthorized access to a business's phone system and typically use it to generate outbound IRSF calls towards revenue share numbers at the victim's expense.

P2S (PIN TO SPEECH) FRAUD

A Wangiri 2.0 fraud scheme scenario. Fraudsters use bots or scripts to stuff an Enterprise`s online form with revenue share numbers, aiming to request one-time passwords (PIN codes). The enterprise then automatically sends these calls to these revenue share numbers which the fraudster will gain revenue from.

WANGIRI

A type of voice fraud where fraudsters make many zero-duration (missed calls) or short duration calls to unkowning subscribers from a revenue share number. The fraudster will gain revenue from those who call back.

WANGIRI 2.0

Fraudsters use bots or scripts to fill out enterprises' online forms with revenue share numbers, to request automatic callbacks either by a robot or an employee.

SPAM

Unsolicited inbound calls to subscribers, including scam calls, nuisance calls or even silent calls. Can be conducted for telemarketing or scam purposes such as from large scale robocallers or unauthroized call centres.

FLASH CALLS

Not considered a fraud scheme but an undesirable traffic type for carriers which seeks replace traditional A2P authenticaion services for one time passwords (OTPs). Flash Calls are zero-duration calls triggered to subscribers who have requested an OTP, where the call's CLI has been manipulated to include the digits of the intended OTP.

AIT SMS

Artificially inflated traffic is a type of fraud where artificial traffic is generated, such as fake requests for one time passwords (OTP's) or fake new user requests that trigger large amounts of one time password A2P messages. These requests cause revenue loss for the Enterprise being targetted, as well as brand and financial distortion to support large amounts of fictitious new users.

IF YOU WOULD LIKE TO RECEIVE REAL-TIME ALERTS FROM US:

Apply

IF YOU WOULD LIKE TO SUBSCRIBE TO OUR WEEKLY REPORTS:

Subscribe

IRSF

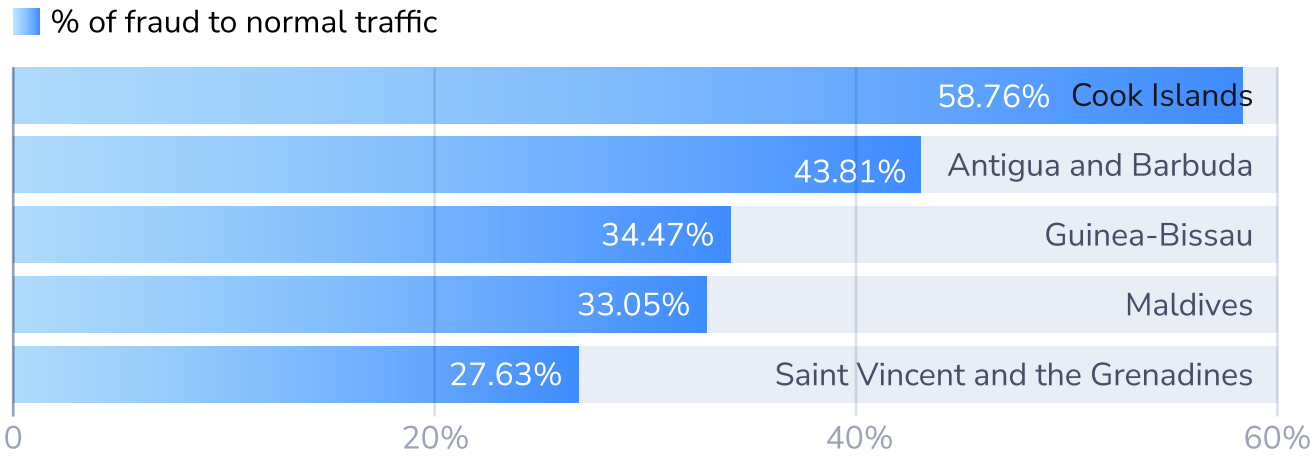
IRSF (International Revenue Share Fraud) typically includes fraudsters artificially driving traffic towards revenue share numbers, which fraudsters gain a profit from. IRSF may also often occur in combination with other fraud types such as Subscription Fraud, Stolen Phones, Roaming events, or most notably in this Q4 report, PBX Hacking which we will also discuss later in the report.

Q4 HIGHLIGHTS

Top country codes for IRSF terminating to them: Cook Islands led with a fraud ratio of 58%, followed by Antigua And Barbuda at 43%, and Guinea-Bissau 34%

The following dashboard identifies the country ranges with the highest ratio of IRSF Fraud to total call attempts terminating to that country range.

TOP FRAUD DESTINATIONS - % FRAUD



WHY IRSF DETECTION REQUIRES MORE THAN STATIC RULES

While certain routes are well known for IRSF activity, fraudsters continually seek opportunities to target less obvious or emerging “hot” destinations. By purchasing revenue share numbers in these locations, attackers can avoid standard rules and threshold-based monitoring, placing greater reliance on a fraud management system’s ability to identify uncommon and evolving patterns.

The Cook Islands provide an illustrative example. As a popular holiday destination, the country can receive legitimate travel-related traffic; however, its numbering ranges also include purchasable revenue share numbers. Q4 showed more than half of all traffic terminating to the Cook Islands was identified as IRSF, a significant proportion for any destination.

This also highlights how perceptions of “normal” traffic can shift throughout the year. Seasonal travel patterns, combined with even a small number of fraud events, can significantly distort averages such as call volumes, durations, and timing. This underlines the need for advanced, AI-driven detection capable of distinguishing genuine changes in traffic behaviour from patterns that clearly match revenue share fraud characteristics.

IRSF – PBX HACKING

UNDERSTANDING IRSF TRAFFIC AND PBX HACKING METHODS

IRSF (International Revenue Share Fraud) typically includes fraudsters artificially driving traffic towards revenue share numbers, which fraudsters gain a profit from. IRSF may also often occur in combination with other fraud types such as Subscription Fraud, Stolen Phones, Roaming events, or PBX Hacking

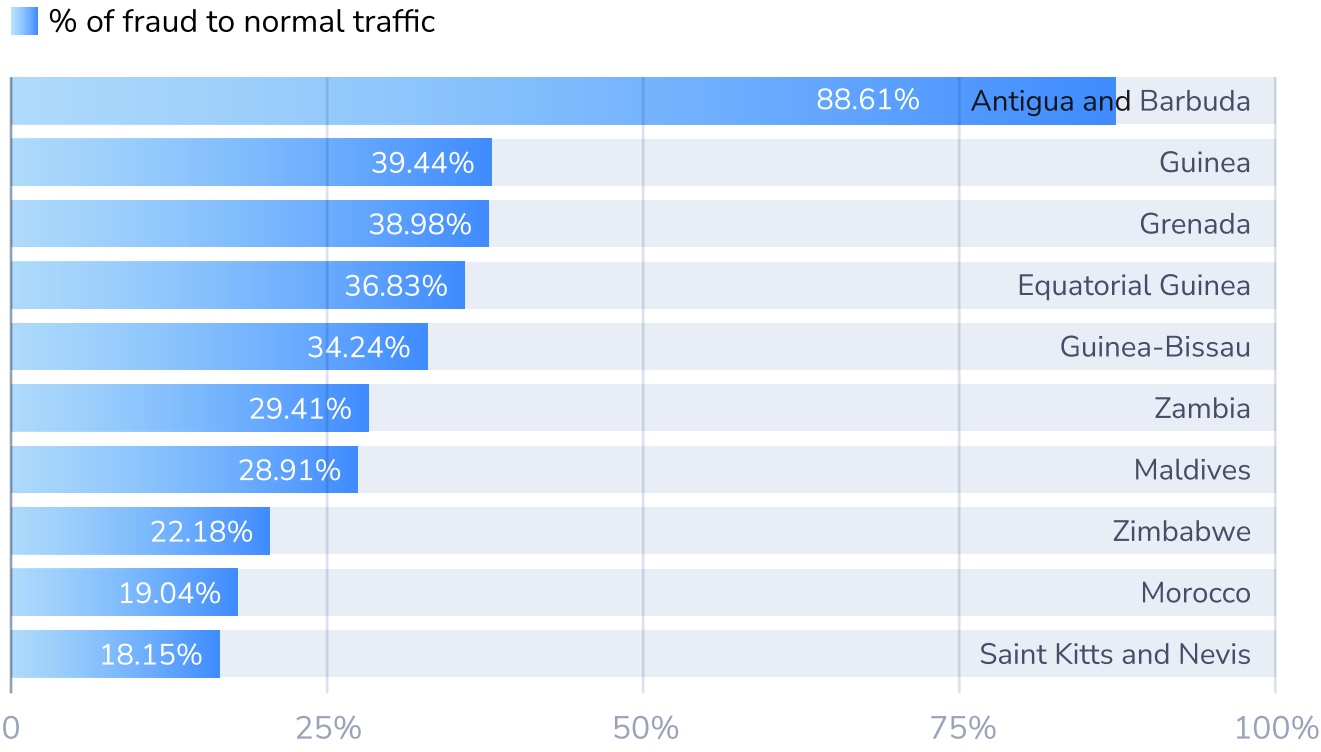
PBX's are often used as a 'fraud method' to commit IRSF, by fraudsters who are able to access badly secured PBX devices inside businesses, and use those to generate artificial traffic towards revenue share numbers. PBX hacking can be identified within typical IRSF attacks as the calls are often timed in one of two ways depending on the business profile: either for the calls to only occur during business hours (so nobody questions who is making calls during the night), or else to only occur outside of business hours (to ensure employees don't notice constant busy lines during their work day).

Q4 HIGHLIGHTS

Top country codes for IRSF terminating to them through PBX Hacking:
Antigua and Barbuda recorded the highest ratio at 88%, followed by Guinea at 39% and Grenada at 3%

The following dashboard identifies the country ranges with the highest ratio of PBX Hacking methods for IRSF to total call attempts terminating to that country range.

TOP FRAUD DESTINATIONS - % FRAUD



IRSF – PBX HACKING

IRSF IMPACT ON LOW-TRAFFIC COUNTRY RANGES

The impact of fraud terminating to a country range that receives relatively little overall traffic is clearly visible in this graph, with 88.61% of traffic to Antigua and Barbuda identified as fraudulent. This destination did not receive high call volumes from our customers during the quarter, which further highlights how pronounced the effect of IRSF attempts can be when they occur.

Operators experiencing IRSF activity may choose to respond by implementing controls such as automatic blocking for the affected country range, showing the need to leverage modern tools to block an attack automatically like what's available within AB Handshake's Fraud Management system, rather than relying on alerts to generate and blocking be performed manually.

P2S

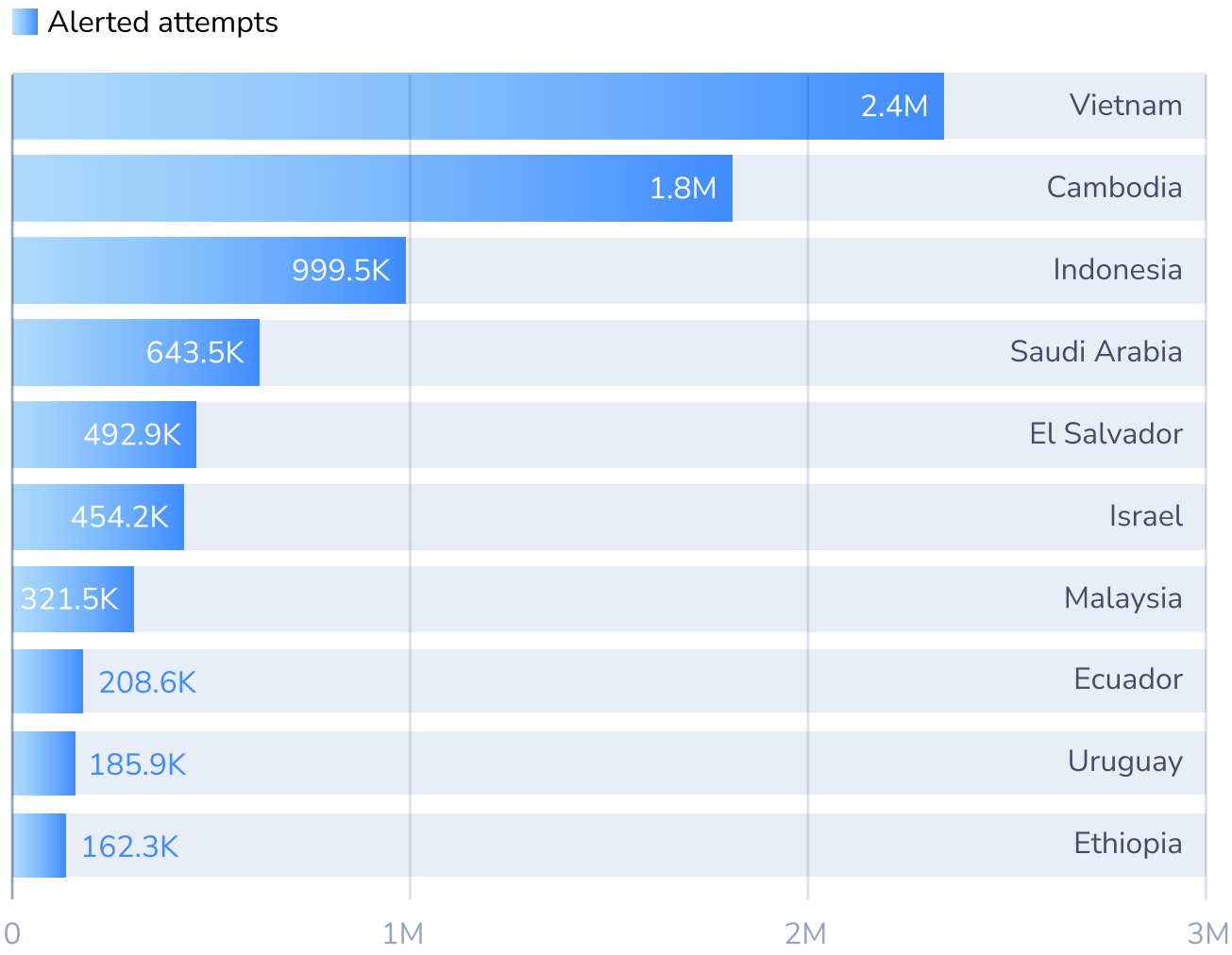
UNDERSTANDING P2S TRAFFIC

P2S attacks typically involve automated bots or scripts abusing web forms or online verification processes to trigger voice-based OTP calls to revenue share numbers, which the fraudsters will gain revenue from. Such patterns often reveal systematic P2S attacks, where repeated automated attempts focus on specific destinations, highlighting them as potential hotspots for this type of revenue share fraud.

Q4 HIGHLIGHTS

Top country ranges for P2S callbacks terminating to them: Vietnam with 2.4 million calls, Cambodia with 1.8 million calls, and Indonesia and almost 1 million calls.

The following dashboard identifies the country ranges receiving the highest level of P2S fraud based on call count.



P2S

P2S FRAUD TRENDS

P2S fraud has been quietly growing in recent periods. Increasingly sophisticated bots potentially enhanced by AI are now capable of targeting large numbers of online verification systems, triggering significant volumes of OTP (one-time password) callbacks to revenue share numbers from which fraudsters gain profit.

With several million calls directed toward the top recipient country ranges in this report alone, the scale of this activity highlights just how significant the problem has become, and why both operators and enterprises need to take action against this type of event.

This trend also suggests that many online systems lack the same level of fraud protection as modern telecom fraud management platforms. As a result, they are likely to be increasingly targeted by P2S attacks. If these systems struggle to identify or defend against well-known high-risk destinations, they will face even greater challenges when fraudsters shift toward more subtle and less obvious country ranges.

WANGIRI

UNDERSTANDING WANGIRI FRAUD

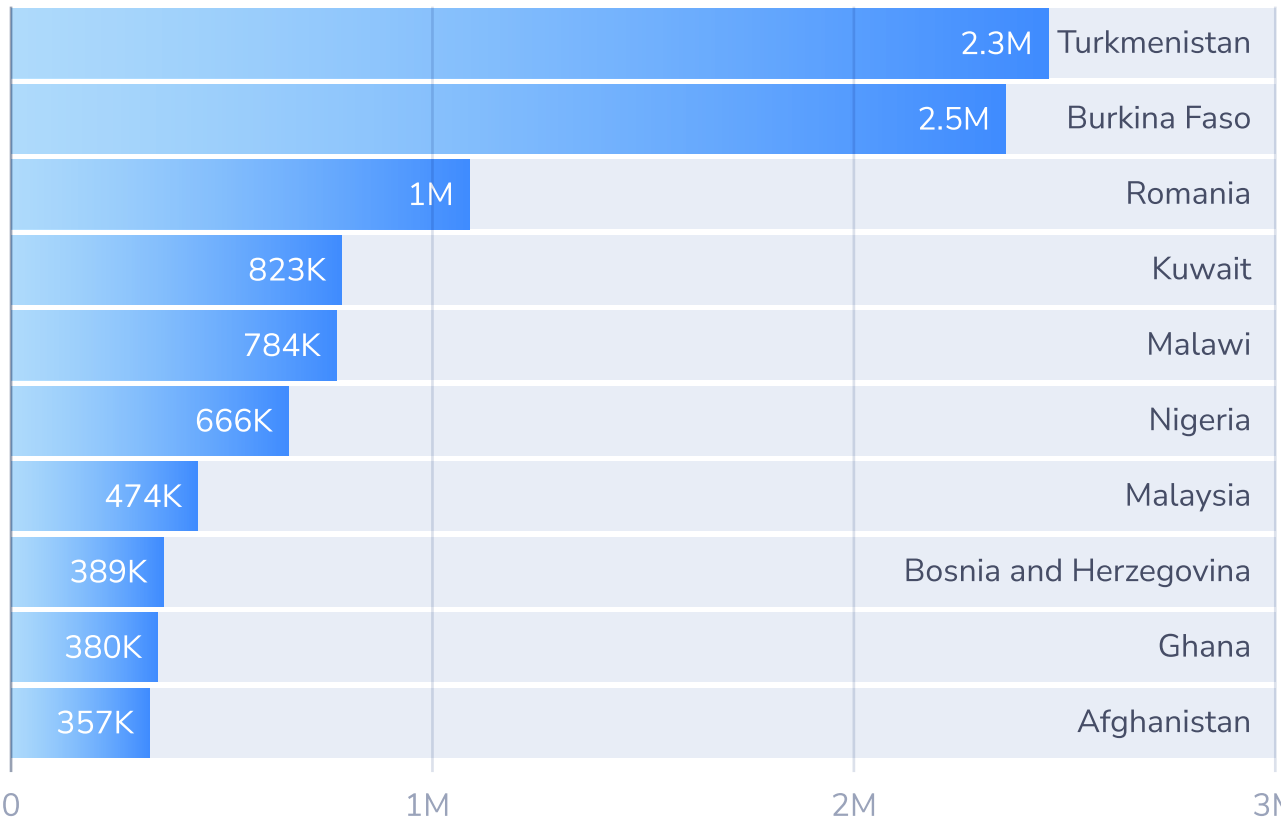
Wangiri fraud works by triggering short one-ring calls or missed calls to users from revenue share numbers, enticing innocent subscribers to call back. Those who do return these calls do not realize they are calling a revenue share number that the fraudster is generating profit from calls to. Other means may be done to entice the caller to stay connected on the line for longer, such as recordings of a phone ringing out, or a long voicemail, etc.

Q4 HIGHLIGHTS

Top country receivers for inbound Wangiri attack calls: Turkmenistan and Burkina Faso at 2 million each, followed by Romania at 1 million.

The following dashboard identifies the country ranges with the highest counts of inbound Wangiri attack calls.

TOP TERMINATION BY INBOUND VOLUME



GLOBAL WANGIRI ACTIVITY AND EMERGING THREATS

Wangiri attacks continue worldwide, with this quarter recording some of the largest attack attempts seen in recent times. As operators and carriers continue to strengthen their defences, fraudsters are increasingly forced to become more creative in their methods to avoid detection.

Wangiri provides an attractive option for fraudsters, as it allows them to target individual subscribers directly. This approach is often far easier to conduct than more traditional IRSF attacks, which typically require access to a SIM card, a compromised device, or other forms of direct network access.

WANGIRI 2.0

UNDERSTANDING WANGIRI 2.0

Wangiri 2.0 typically involves automated systems or bots that submit revenue share numbers through online forms, triggering automated callbacks from enterprises or applications.

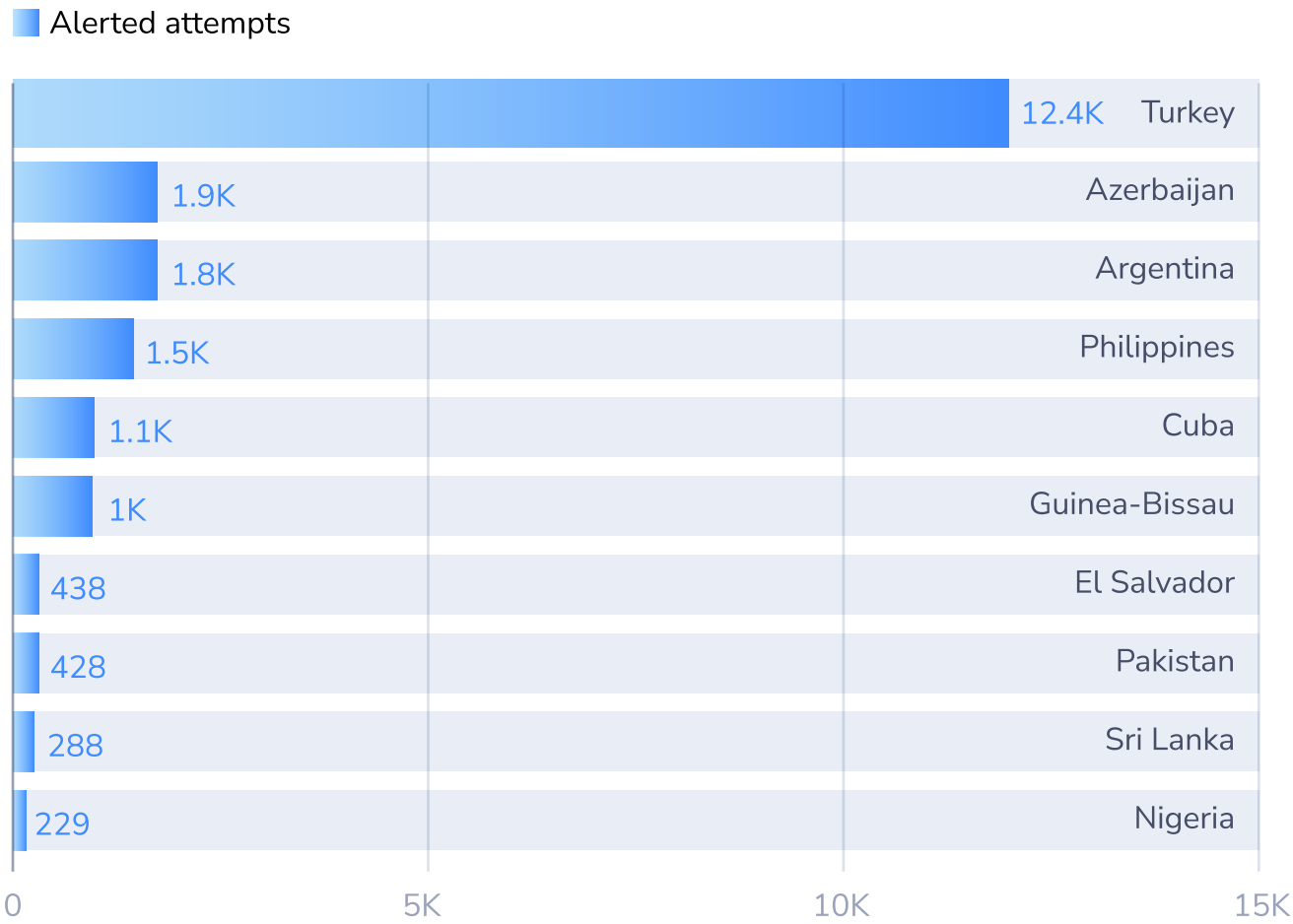
These callbacks are then monetized by keeping the line active, often using ringing tones or recorded loops to extend call duration and entice the caller to ‘stay on the line’.

Q4 HIGHLIGHTS

Top country codes for terminating Wangiri 2.0 calls: Turkey 12.4k, Azerbaijan with 2k, and Argentina with 1.8k.

The following dashboard identifies the country code ranges with the highest calls from Wangiri 2.0 sources.

TOP TERMINATION BY OUTBOUND VOLUME %



WANGIRI 2.0

WANGIRI 2.0 FRAUD TRENDS

Wangiri 2.0 is showing high levels of activity across a wide range of country codes globally. Where fraudsters once needed to target individual subscriber MSISDNs, they can now simply submit revenue share numbers through online forms and automatically trigger callbacks from enterprises or applications, effectively guaranteeing a return call.

This quarter, we observed significant volumes terminating to Turkish Range, a destination not traditionally associated with revenue share fraud. This may signal a broader shift in fraudster behaviour, as attackers increasingly select more diverse and less obvious destinations in an effort to stay ahead of detection.

SPAM

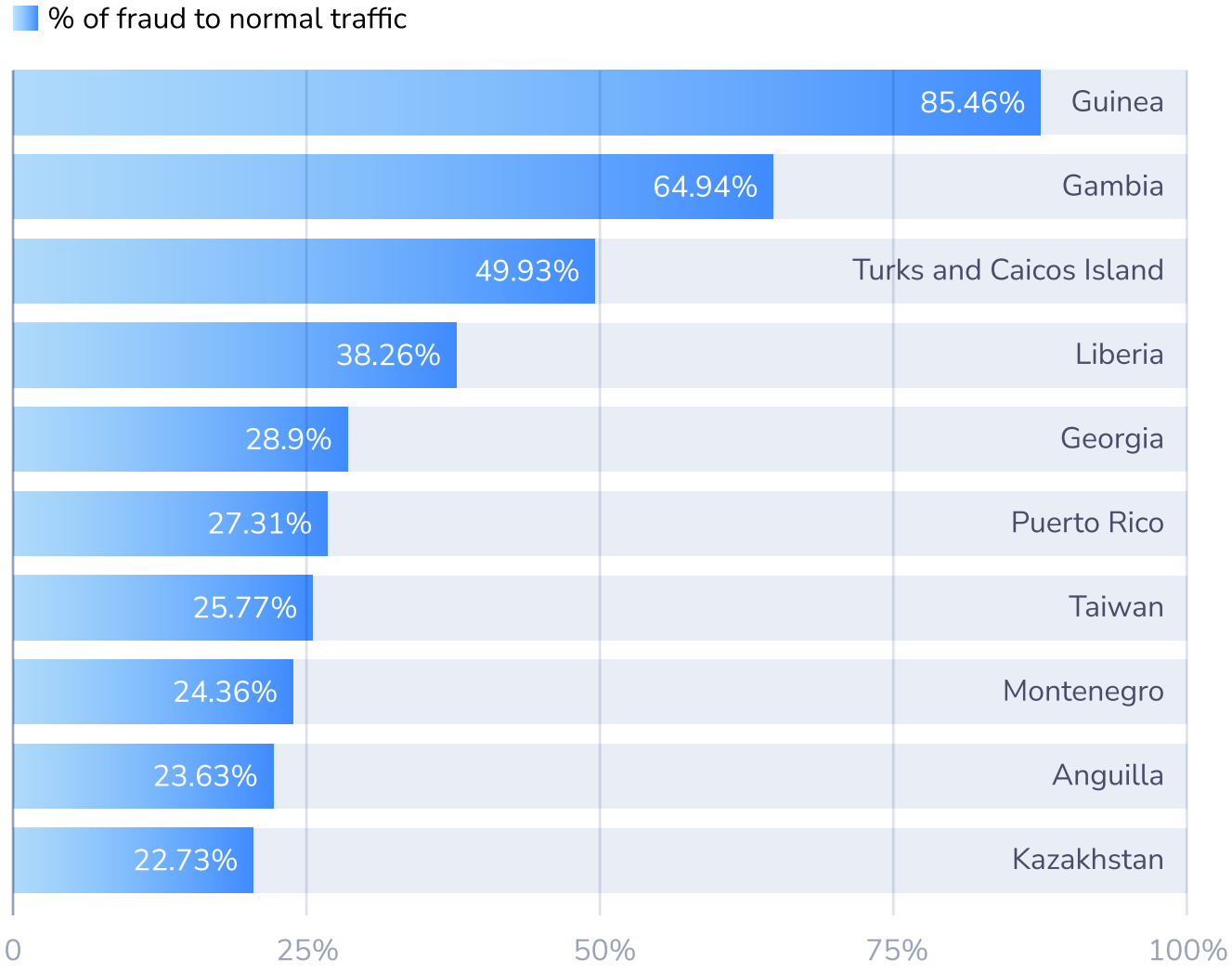
UNDERSTANDING SPAM TRAFFIC

Spam traffic typically includes unsolicited robocalls or auto-dialed messages, often used for advertising, scamming, or phishing.

Q4 HIGHLIGHTS

Top receivers for inbound spam: Guinea lead with 85%, followed by Gambia at 65% and Turks and Caicos Islands at 50%.

TOP FRAUD DESTINATIONS - % FRAUD TRAFFIC



RISING SPAM VOLUMES AND VALIDATION STRATEGIES

No one is surprised to see spam calls continuing to grow, but so too are the methods used to detect them, driven by increasingly advanced AI tools and techniques. Operators, however, are often constrained by the inability to confirm a call's content or authenticity, limiting their ability to take decisive action.

This lack of intervention allows spam traffic to persist, leading to higher call volumes and declining pick-up rates, which in turn erodes trust in the authenticity of calls across the network.

Against this backdrop, AB Handshake's Call Validation Technology provides a powerful solution. By enabling operators and enterprises to verify the authenticity of each call or SMS and confirm that it is genuinely from the stated origin, trust can be restored and fraudulent traffic effectively challenged.

FLASH CALLS

UNDERSTANDING FLASH CALLS

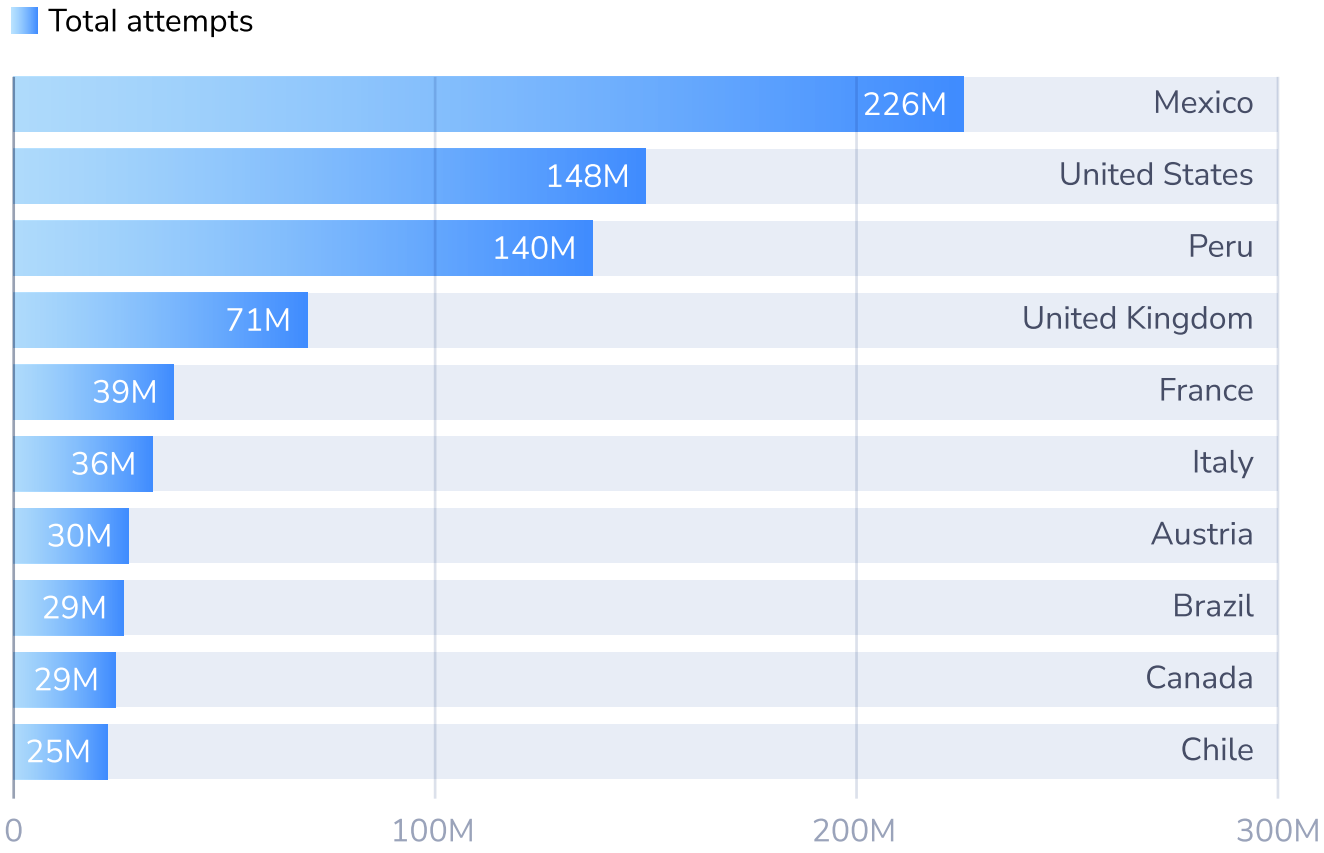
Flash calls are often used for rapid one time password or two factor authentication (app sign-ins, one time password delivery) in place of traditional . Fraudsters abuse this mechanism to generate silent calls at scale or to farm responses from carriers and APIs.

Q4 HIGHLIGHTS

- Originating Country Code Ranges: Mexico leads with an overwhelming 226M total attempts, followed by the United States 148M and Peru 140M.
- Terminating Country Code Ranges: Mexico leads with an overwhelming 203M Total attempts, followed by Peru 140M and Bangladesh 63M.
- Top 10 Destinations with Local Numbers: Mexico leads with an overwhelming 223M attempts, followed by Peru 139M and the United Kingdom 34M.

The following dashboard identifies the country ranges with the highest levels of Flash Calls originating from them

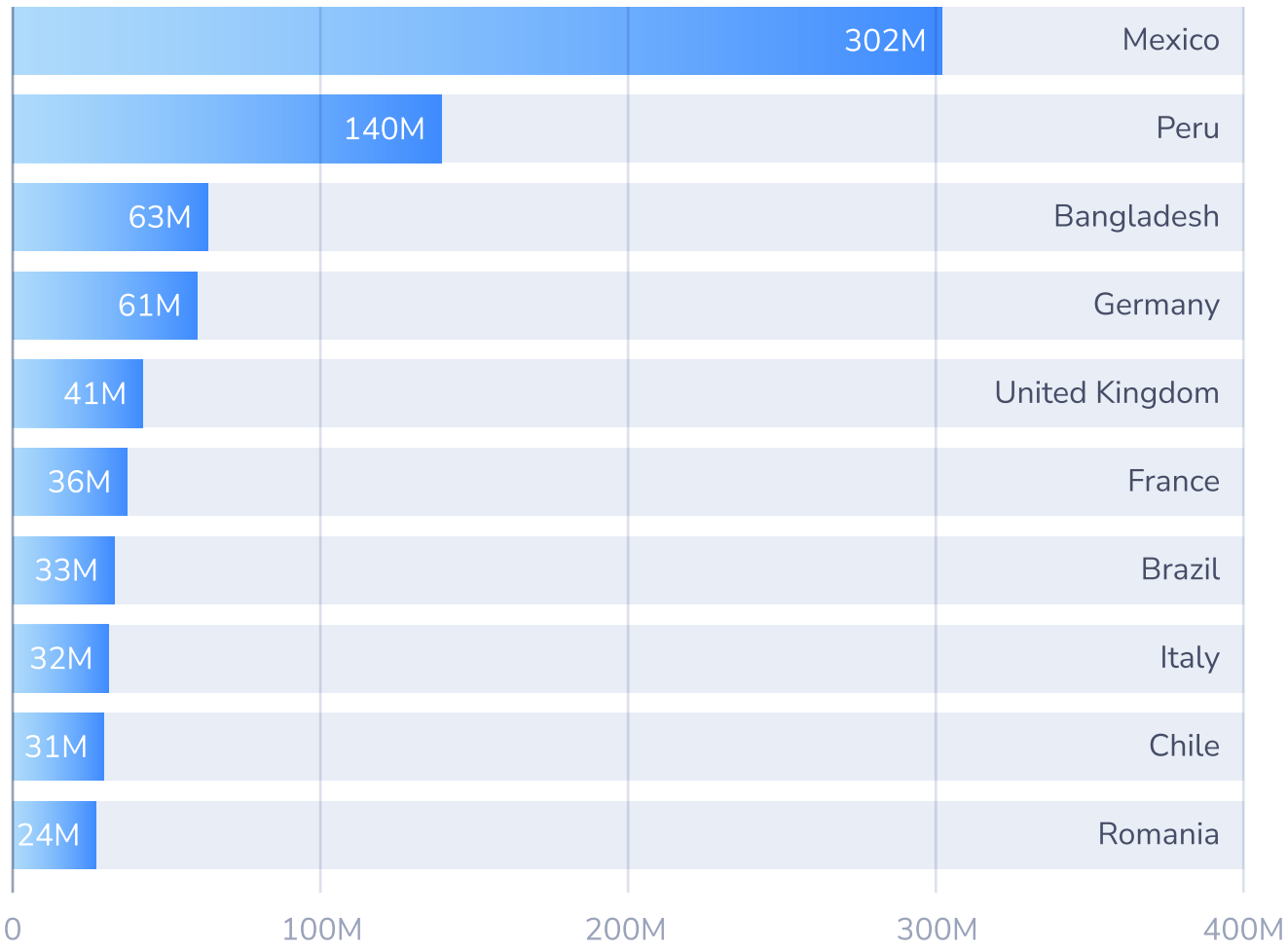
TOP ORIGINATING COUNTRIES BY VOLUME



FLASH CALLS

The following dashboard identifies the country ranges with the highest levels of Flash Calls terminating to them

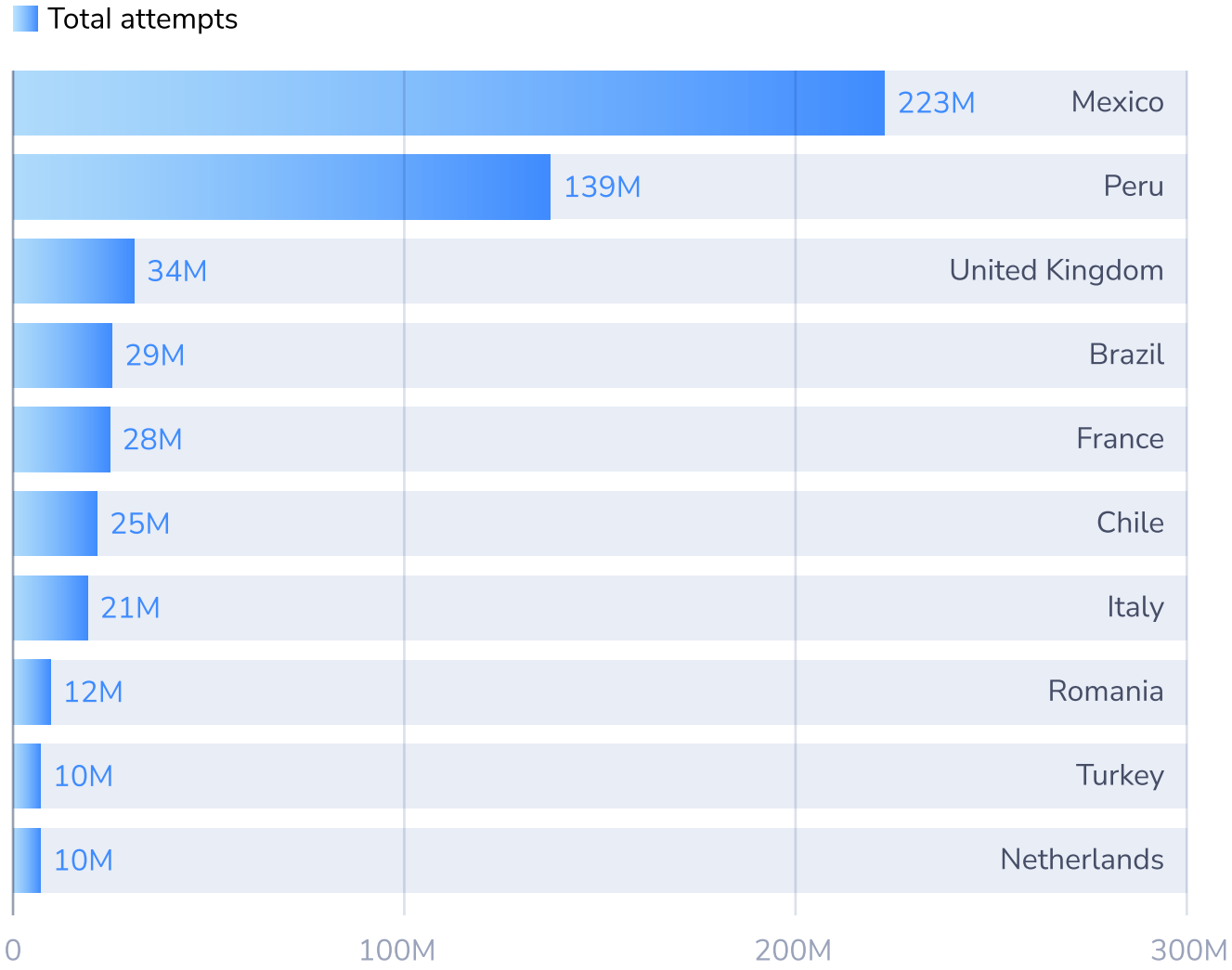
TOP TERMINATION COUNTRIES BY VOLUME



FLASH CALLS

The following dashboard identifies the country code ranges with the highest levels of local Flash Calls originating from and terminating to them

TOP DESTINATIONS - LOCAL



WHAT THE DATA TELLS US

Flash Calls continue to grow, with hundreds of millions of attempts identified in the last quarter alone. This scale clearly highlights the urgent need for operators to respond. As the A2P market continues to redefine itself amid increasingly challenging conditions, operators are under growing pressure to act now.

SMS AIT

UNDERSTANDING SMS AIT TRAFFIC

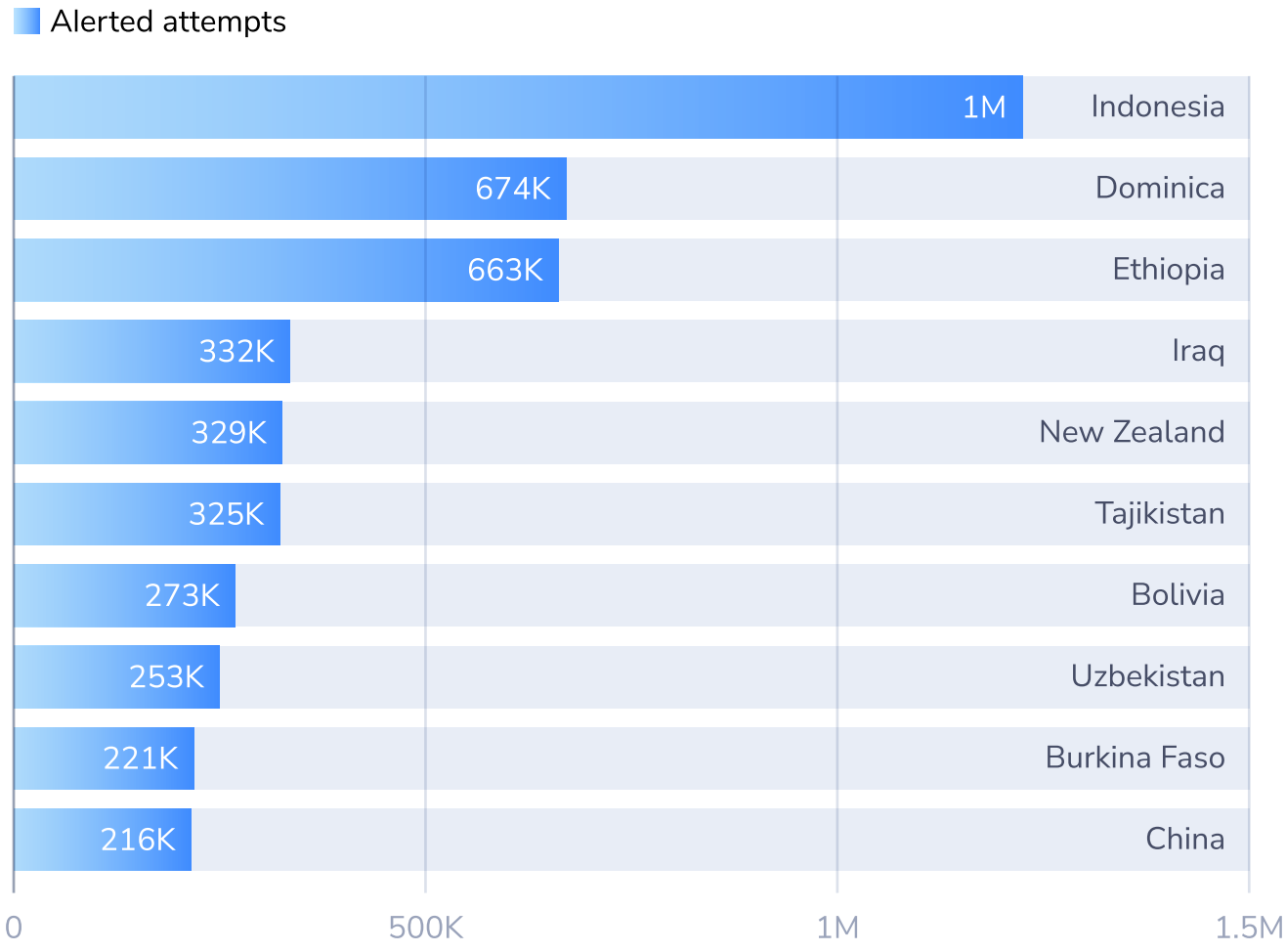
This section highlights the top 10 country code ranges where SMS AIT (Artificial Inflation of Traffic) messages were most frequently terminated i.e., where the artificial A2P SMS's were delivered during the quarter. High termination volumes suggest that these ranges are being used as endpoints for artificially inflated SMS activity, often with no legitimate user behind the traffic.

Q4 HIGHLIGHTS

Top SMS AIT Country ranges: Indonesia leads with 1 million, Dominica 674 K, and Ethiopia with 663K.

The following dashboard identifies the country ranges with the highest level of SMS AIT terminating to them.

TOP SMS AIT FRAUD TARGET COUNTRIES (ALERTED)



SMS AIT: EMERGING DESTINATIONS AND OPERATOR CHALLENGES

We see several surprising entries on this list, including Iraq, which typically does not receive large volumes of international traffic and would not normally appear on hot destination lists for telecom fraud. New Zealand also appears, despite not being associated with any established high-risk country databases for fraudulent traffic.

This could potentially indicate that SMS AIT fraudsters have yet to be meaningfully challenged in a way that forces them to conceal or diversify their activity. As a result, there is little incentive for them to hide this traffic at all.

While many fraud management systems remain unable to detect SMS AIT, even when volumes spike sharply toward well-known high-risk destinations, AB Handshake's system is able to identify this activity and expose the full extent of its impact on enterprises.

Q4 DISCUSSION TOPIC: SMS AIT IS NO LONGER HIDING, AND THAT'S THE MOST DANGEROUS SIGN OF ALL

SMS AIT (Artificial Inflation of Traffic) is one of the most structurally damaging fraud types in the telecom ecosystem. Unlike spam or phishing, its goal is not to deceive an end user, but to silently manufacture large volumes by generating large quantities of SMS traffic with no legitimate recipient and no genuine business purpose.

AB Handshake's detections this quarter delivered some of the strongest indicators yet that SMS AIT activity is continuing to expand.

What stands out is not just the scale of this activity, but the lack of disguise. These campaigns are not attempting to blend into traffic or mask themselves with low-and-slow behaviour. Instead, they appear increasingly confident that many networks still lack the tooling required to effectively challenge them.

The most concerning trend in Q4 is that fraudsters no longer feel pressure to hide SMS AIT activity. In contrast to voice fraud where attackers constantly adapt destinations, timing, and patterns to evade controls, SMS AIT commonly presents with the following characteristics:

- Concentrated delivery into specific country ranges
- Repetitive and predictable routing paths
- Sustained high volumes
- No corresponding user engagement

This points to a troubling reality: in many environments, SMS AIT remains effectively invisible unless operators and enterprises are using AI-enhanced fraud detection systems, such as AB Handshake's. SMS AIT is uniquely dangerous because it exploits trust between systems, not people, and has vast effects on revenue. Even more concerning is the emergence of unexpected country range destinations. When countries with historically low international SMS demand suddenly receive large volumes of inflated traffic, it highlights how heavily many fraud strategies still rely on static hotlists rather than adaptive, AI driven detection. Traditional controls struggle because they focus on message content or sender IDs, and without real-time visibility into destination risk, traffic intent, and historical patterns, inflated traffic can appear deceptively normal.

WHAT SUCCESS LOOKS LIKE AND HOW WE GET THERE

Stopping SMS AIT requires a fundamental shift in approach: moving beyond basic filtering toward AI-enhanced fraud detection, combined with real-time validation capabilities. AB Handshake's SMS Validation technology is based on cross-validation of each SMS directly between originating and terminating enterprises or operators via an out-of-band channel. Based on this validation, traffic can be blocked or allowed to proceed without intervention.

AB HANDSHAKE

WANT TO GET EVEN MORE DATA?

Subscribe for weekly reports to see the full picture, including A and B number ranges for all attacks.

Or, sign-up for real-time alerts and block the fraudulent destinations for the duration of the attack. **Don't be a victim of voice fraud!**

CONTACT US

ADDRESS
66 West Flagler Street, Suite 900 — #2329, Miami, FL, USA, 33130

EMAIL
contact@abhandshake.com

ABHANDSHAKE.COM